

(43)公開日 平成10年(1998)9月11日

310K

審査請求 未請求 請求項の数9 OL (全 22 頁)

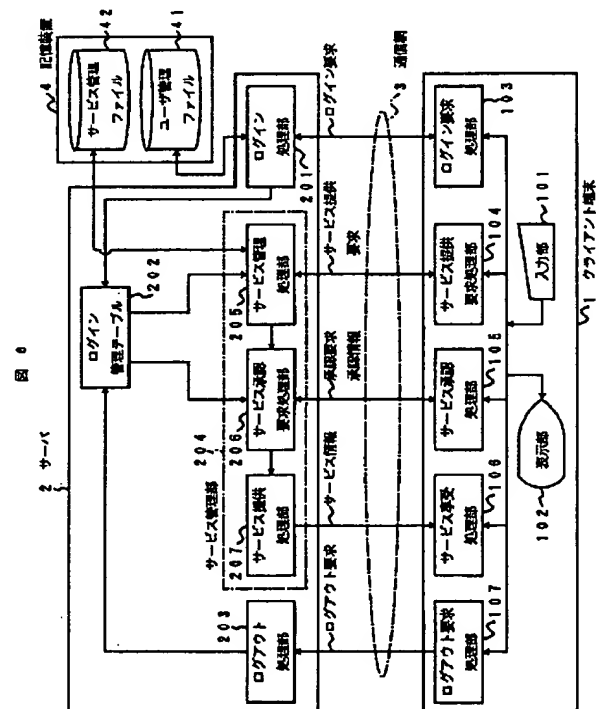
最終頁に続く

(54) 【発明の名称】 クライアント・サーバシステム、サーバおよびクライアント端末

(57) 【要約】

【課題】サービスの利用に際して他のユーザの承認が必要な場合でも、ユーザのサービスへのアクセス管理を適正に行うことを目的とする。

【解決手段】 サーバ2は、まず、クライアント端末2から送られてきたユーザ識別子及びパスワードと、自己が備えるユーザ管理ファイル202とを用いてログイン処理を行う。次に、クライアント端末1から送られてきたサービス提供要求と、自己が備えるサービス管理ファイル42とを用いてサービス管理を行う。サービス提供に際し他のユーザに承認を得る必要であると判断した場合は、当該ユーザが使用するクライアント端末1に承認要求を行う。当該承認要求に対する応答が承認許諾の場合は、前記サービス提供要求に応じた処理を行う。承認拒否の場合は、その旨を前記サービス提供要求を行ったユーザに通知する。



【特許請求の範囲】

【請求項 1】 少なくとも 1 つのクライアント端末と、前記クライアント端末に少なくとも 1 つのサービスを提供する少なくとも 1 つサーバと、からなるクライアント・サーバシステムであって、

前記サーバは、前記少なくとも 1 つのサービス各々について、前記クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報を特定するための承認条件と、の対応関係を示す管理テーブルが記憶された管理テーブル記憶手段と、

前記少なくとも 1 つサービスの前記クライアント端末への提供を管理するサービス提供管理手段と、を備え、前記クライアント端末は、ユーザの識別情報の入力や、前記サーバが提供するあるサービスについてのサービス提供要求といった、当該クライアント端末を利用しているユーザの指示を受け付ける入力手段と、

前記入力手段で受け付けた前記ユーザの指示を、前記サーバに送信する送信手段と、を備え、

前記サービス提供管理手段は、前記クライアント端末から送信された、当該クライアント端末を利用しているユーザの前記サービス提供要求によって特定されるサービスについて、当該ユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報に対応付けられた承認条件を、前記管理テーブル記憶手段から検索する承認条件検索手段と、

前記承認条件検索手段で検出した承認条件が、承認を必要としない旨を示している場合は、当該サービス提供要求に応じた処理を実行し、承認を必要とする旨を示している場合は、当該承認条件によって定まるユーザの識別情報を有するユーザの承認を受けた後に、当該サービス提供要求に応じた処理を実行するサービス提供実行手段と、

を備えていることを特徴とするクライアント・サーバシステム。

【請求項 2】 請求項 1 記載のクライアント・サーバシステムにおいて、

複数の前記クライアント端末を有し、

前記サービス提供管理手段は、複数の前記クライアント端末各々から送られたきた、当該クライアント端末を使用するユーザの識別情報を、当該クライアント端末の識別情報に対応付けて記憶する識別情報記憶手段と、

前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合に、当該承認条件によって定まるユーザの識別情報に対応付けられたクライアント端末の識別情報を、前記識別情報記憶手段から検索する識別情報検索手段と、

前記識別情報検索手段で検出されたクライアント端末の

識別情報によって特定されるクライアント端末に、前記サービス提供要求を送信したクライアント端末のユーザが、当該サービス提供要求を行った旨を通知する通知手段と、をさらに備え、

前記入力手段は、前記通知手段により通知されたサービス提供要求に応じた処理の承認を行うか否かを特定するための承認許諾情報の入力をも受け付けるものであり、前記サービス提供実行手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合において、前記識別情報検索手段で検出されたクライアント端末の識別情報によって特定されるクライアント端末から送信された前記承認許諾情報が、前記サービス提供要求に応じた処理の承認を行う旨を示している場合にのみ、当該サービス提供要求に応じた処理を実行するものである、

ことを特徴とするクライアント・サーバシステム。

【請求項 3】 請求項 2 記載のクライアント・サーバシステムであって、

前記通知手段は、さらに、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合であって、当該承認条件によって定まるユーザの識別情報が前記識別情報記憶手段に複数記憶されている場合に、当該複数のユーザの識別情報を前記サービス提供要求を送信したクライアント端末に通知するものであり、

前記入力手段は、前記通知手段により通知された複数のユーザの識別情報のなかから、少なくとも 1 つを選択するための選択情報の入力をも受け付けるものであり、前記識別情報検索手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合であって、当該承認条件によって定まるユーザの識別情報が前記識別情報記憶手段に複数記憶されている場合には、前記サービス提供要求を送信したクライアント端末から送信された、前記選択情報によって定まるユーザの識別情報に対応付けられたクライアント端末の識別情報を、前記識別情報記憶手段から検索するものである、

ことを特徴とするクライアント・サーバシステム。

【請求項 4】 請求項 2 記載のクライアント・サーバシステムであって、

前記サービス提供管理手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合であって、当該承認条件によって定まるユーザの識別情報が前記識別情報記憶手段に複数記憶されている場合に、少なくとも 1 つのユーザの識別情報を前記識別情報記憶手段から選択する選択手段を、さらに有し、

前記識別情報検索手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合であって、当該承認条件によって定まるユーザの識別情報が前記識別情報記憶手段に複数記憶されている場合は、前記選択手段で選択された識別情報に対応付けられたクライアント端末の識別情報を、前記識別情報記憶手段か

ら検索するものであること、
を特徴とするクライアント・サーバシステム。

【請求項 5】請求項 2、3 又は 4 記載のクライアント・サーバシステムであって、
前記サービス提供管理手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合であって、当該承認条件によって定まるユーザの識別情報が前記識別情報記憶手段に記憶されていない場合に、当該ユーザの識別情報を一時記憶する識別情報一時記憶手段をさらに有し、
前記識別情報検索手段は、前記識別情報一時記憶手段にユーザの識別情報が一時記憶されている場合、当該ユーザの識別情報が前記識別情報記憶手段に記憶されたときに、当該ユーザの識別情報に対応付けられたクライアント端末の識別情報を、前記識別情報記憶手段から検索するものであること、
を特徴とするクライアント・サーバシステム。

【請求項 6】少なくとも 1 つのクライアント端末と、前記クライアント端末に少なくとも 1 つのサービスを提供する第一のサーバと、前記第一のサーバを管理する第二のサーバと、からなるクライアント・サーバシステムであって、
前記第二のサーバは、前記少なくとも 1 つのサービス各々について、前記クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報を特定するための承認条件と、の対応関係を示す管理テーブルが記憶された管理テーブル記憶手段と、
前記少なくとも 1 つサービスの前記クライアント端末への提供を管理するサービス提供管理手段と、を備え、
前記クライアント端末は、ユーザの識別情報の入力や、前記サーバが提供するあるサービスについてのサービス提供要求といった、当該クライアント端末を利用しているユーザの指示を受け付ける入力手段と、
前記入力手段で受け付けた前記ユーザの指示を、前記第二のサーバに送信する指示送信手段と、を備え、
前記サービス提供管理手段は、前記クライアント端末から送信された、当該クライアント端末を利用しているユーザの前記サービス提供要求によって特定されるサービスについて、当該ユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報に対応付けられた承認条件を、前記管理テーブル記憶手段から検索する承認条件検索手段と、
前記承認条件検索手段で検出した承認条件が、承認を必要としない旨を示している場合は、当該サービス提供要求に応じた処理を実行するように前記第一のサーバを制御し、承認を必要とする旨を示している場合は、当該承認条件によって定まるユーザの識別情報を有するユーザ

の承認を受けた後に、当該サービス提供要求に応じた処理を実行するように、前記第一のサーバを制御する第一のサーバ制御手段と、

を備えていることを特徴とするクライアント・サーバシステム。

【請求項 7】クライアント端末に少なくとも 1 つのサービスを提供するサーバであって、
前記少なくとも 1 つのサービス各々について、前記クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報を特定するための承認条件と、の対応関係を示す管理テーブルが記憶された管理テーブル記憶手段と、

前記少なくとも 1 つサービスの前記クライアント端末への提供を管理するサービス提供管理手段と、を備え、
前記サービス提供管理手段は、前記クライアント端末から送信された、あるサービスについてのサービス提供要求について、当該クライアント端末の識別情報、あるいは当該識別情報によって定まるユーザのレベル情報に対応付けられた承認条件を、前記管理テーブル記憶手段から検索する承認条件検索手段と、

前記承認条件検索手段で検出した承認条件が、承認を必要としない旨を示している場合は、当該サービス提供要求に応じた処理を実行し、承認を必要とする旨を示している場合は、当該承認条件によって定まるユーザの識別情報を有するユーザの承認を受けた後に、当該サービス提供要求に応じた処理を実行するサービス提供実行手段と、

を備えていることを特徴とするサーバ。

【請求項 8】請求項 7 記載のサーバにおいて、
前記サービス提供管理手段は、複数の前記クライアント端末各々から送られたきた、当該クライアント端末を使用するユーザの識別情報を、当該クライアント端末の識別情報に対応付けて記憶する識別情報記憶手段と、
前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合に、当該承認条件によって定まるユーザの識別情報に対応付けられたクライアント端末の識別情報を、前記識別情報記憶手段から検索する識別情報検索手段と、

前記識別情報検索手段で検出されたクライアント端末の識別情報によって特定されるクライアント端末に、前記サービス提供要求を送信したクライアント端末のユーザが、当該サービス提供要求を行った旨を通知する通知手段と、をさらに備え、

前記サービス提供実行手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合において、前記識別情報検索手段で検出されたクライアント端末の識別情報によって特定されるクライアント

端末から、前記サービス提供要求に応じた処理の承認を行う旨を示す承認許諾情報が送信された場合にのみ、当該サービス提供要求に応じた処理を実行するものである、

ことを特徴とするサーバ。

【請求項 9】ユーザの識別情報の入力や、サーバが提供するあるサービスについてのサービス提供要求といった、当該クライアント端末を利用しているユーザの指示を受け付ける入力手段と、前記入力手段で受け付けた前記ユーザの指示を、前記サーバに送信する送信手段とを備え、

前記サーバから提供されたサービスを享受するクライアント端末であって、

前記サーバから通知された、他のクライアント端末のユーザが行ったサービス提供要求に関する情報を表示する表示手段を有し、

前記入力手段は、前記表示手段により表示された、他のクライアント端末のユーザが行ったサービス提供要求について、前記サーバで当該サービス提供要求に応じた処理を実行するために必要な承認の入力をも受け付けるものである、

ことを特徴とするクライアント端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クライアント・サーバシステムに関し、特に、サーバがクライアント端末に提供する各種サービスについて、クライアント端末利用者の当該サービスへのアクセス権を管理することができるクライアント・サーバシステム、および当該システムを構成するサーバ及びクライアント端末に関する。

【0002】

【従来の技術】近年、情報通信機器の発達により、ワークステーションやパソコン等の端末を相互に接続したローカルエリアネットワーク（LAN）が普及している。これに伴い、コンピュータの利用形態も、スタンドアロン型からクライアント・サーバ型へと移行しつつある。

【0003】クライアント・サーバシステムは、スタンドアロン型に比べ、複数のユーザ（クライアント端末利用者）による協調作業を容易に実現することができ、また、高度な処理能力を必要とする作業をサーバに行わせることで、クライアント端末に上記のような処理能力が要求されず、コストパフォーマンスがよいなどの利点を有する。

【0004】しかしながら、クライアント・サーバシステムでは、複数のユーザがクライアント端末を介してサーバを利用することになるので、機密漏洩や情報改竄など不正を防ぐため、サーバがクライアント端末を介してユーザに提供する各種サービスについて、ユーザの当該サービスへのアクセスを管理する必要がある。

【0005】従来のクライアント・サーバシステムにお

いて、上記アクセスの管理は、通常、サーバのオペレーティング・システム（OS）が、アクセス・コントロールリストと呼ばれる管理テーブルを利用して、ディレクトリやファイルに対するアクセスをユーザ毎、あるいはプログラム毎に制限することで行っている。

【0006】このアクセス・コントロールリストを利用して、ユーザのアクセスを管理する方法については、たとえば「暗号とデータセキュリティ」（著者：D. E. R. デニング、訳者：上園 忠弘、小嶋 格、奥島 晶子、発行元：培風館）に記載されている。この文献での記載を簡単に説明すると、以下のものである。

【0007】システムの状態を、能動的なエンティティである主体 s （サブジェクト）の集合 S と、システムで保護されるエンティティである対象 o （オブジェクト）の集合 O と、読み取りや書き込み、あるいは実行といった個々のアクセス権の組み合わせ r の集合 R とで定義する。

【0008】各対象 o_i に対するアクセスを、アクセス・コントロールリスト $o_i[s_j, r_j]$ によって制御する。

【0009】ここで、 $0 < i \leq n$ 、 $0 < j \leq m$ である。ただし、 n は集合 O の要素数（対象 o の総数）、 m は集合 S の要素数（主体 s の総数）である。

【0010】たとえば、対象 o_k （ここで、 k は、 $0 < k \leq n$ を満たす定数とする）が F というファイルであり、対象 o_k に対して、 o_k [ユーザ A , 読み取り] というアクセス・コントロールリストと、 o_k [ユーザ B , 読み取り・書き込み・実行] というアクセス・コントロールリストとが設定されていると仮定する。

【0011】この場合、サーバは、ユーザ B に対しては、ファイル F について読み取り、書き込み、および実行という三種類のアクセスを許可するが、ユーザ A に対しては、ファイル F について読み取りという種類のアクセスのみを許可し、その他のアクセスを許可しない。

【0012】

【発明が解決しようとする課題】上記従来のアクセス・コントロールリストを用いてユーザのアクセスを管理するクライアント・サーバシステムでは、サーバ管理者がサーバに前記アクセス・コントロールリストを設定することで、サーバに、ユーザの当該サーバが提供する各種サービスへのアクセスを管理させている。

【0013】ところで、企業などの組織において、ある業務処理を行おうとする場合、当該業務処理の担当者は、事前に上司の承認を得ておかなければならない場合が多々ある。あるいは、同じ業務処理を担当する複数の同僚に、事前に同意を得ておかなければならない場合も考えられる。

【0014】このことは、クライアント・サーバシステムを利用する場合にも、同様に起こり得る。すなわち、ユーザが、クライアント端末を介して、サーバが提供す

るあるサービスを利用しようとする場合、当該ユーザは、事前に他のユーザの承認や同意を得ておかなければならない場合がある。

【0015】このような場合、上記従来のアクセス・コントロールリストを用いてユーザのアクセスを管理するクライアント・サーバシステムでは、あるオブジェクト（たとえばファイル）に対して、当該システムを利用する複数のユーザ（サブジェクト）各々が、どのようなアクセス権限（読み取り、書き込み、実行等）を持っているかということのみを、アクセス管理の判定条件としているので、以下のような問題が生じる。

【0016】①アクセス・コントロールリストが前記ユーザのサービス利用を許可するように設定されている場合、当該ユーザは、事前に他のユーザの承認や同意を得るのを忘れて、当該サービスにアクセスするおそれがある。これでは、ユーザのアクセス管理を適正に行うことができない。

【0017】②アクセス・コントロールリストが前記ユーザのサービス利用を許可しないように設定されている場合、当該ユーザは、事前に承認あるいは同意を得たことをサーバ管理者に通知して、一時期、前記サービスを利用できるように、アクセス・コントロールリストを変更してもらうなどの手続きが必要になる。このため、ユーザおよびサーバ管理者に負担がかかる。

【0018】このように、上記従来のクライアント・サーバシステムでは、クライアント端末利用者であるユーザが、サーバが提供するあるサービスを利用する場合において、他のユーザの承認や同意が必要な場合には、当該ユーザの前記サービスへのアクセス管理を適正に行うことができない。

【0019】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、クライアント端末利用者であるユーザが、サーバが提供するあるサービスを利用する場合において、他のユーザの承認や同意が必要な場合であっても、当該ユーザの前記サービスへのアクセス管理を適正に行うことができるクライアント・サーバシステム、サーバおよびクライアント端末を提供することにある。

【0020】

【課題を解決するための手段】上記課題を達成するために、本発明のクライアント・サーバシステムは、少なくとも1つのクライアント端末と、前記クライアント端末に少なくとも1つのサービスを提供する少なくとも1つのサーバと、からなるクライアント・サーバシステムであって、前記サーバは、前記少なくとも1つのサービス各々について、前記クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報

を特定するための承認条件と、の対応関係を示す管理テーブルが記憶された管理テーブル記憶手段と、前記少なくとも1つのサービスの前記クライアント端末への提供を管理するサービス提供管理手段と、を備え、前記クライアント端末は、ユーザの識別情報の入力や、前記サーバが提供するあるサービスについてのサービス提供要求といった、当該クライアント端末を利用しているユーザの指示を受け付ける入力手段と、前記入力手段で受け付けた前記ユーザの指示を、前記サーバに送信する送信手段と、を備え、前記サービス提供管理手段は、前記クライアント端末から送信された、当該クライアント端末を利用しているユーザの前記サービス提供要求によって特定されるサービスについて、当該ユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報に対応付けられた承認条件を、前記管理テーブル記憶手段から検索する承認条件検索手段と、前記承認条件検索手段で検出した承認条件が、承認を必要としない旨を示している場合は、当該サービス提供要求に応じた処理を実行し、承認を必要とする旨を示している場合は、当該承認条件によって定まるユーザの識別情報を有するユーザの承認を受けた後に、当該サービス提供要求に応じた処理を実行するサービス提供実行手段と、を備えていることを特徴とする。

【0021】本発明のクライアント・サーバシステムでは、サーバが提供するサービス各々について、クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報を特定するための承認条件と、の対応関係を示す管理テーブルを管理テーブル記憶手段に格納している。

【0022】そして、あるクライアント端末から、サーバが提供するあるサービスに対するサービス提供要求があった場合、当該クライアント端末を使用しているユーザの識別情報、あるいは当該識別情報で定まるユーザのレベル情報に対応付けられた承認条件を、前記管理テーブルから検索している。

【0023】その後、検出した承認条件が、前記サービス提供要求に応じた処理を行うのに承認が必要であることを示している場合は、当該承認条件によって定まる識別情報を有するユーザの承認を受領を条件として、当該サービス提供要求に応じた処理の実行を行うようにしている。

【0024】したがって、本発明によれば、クライアント端末利用者であるユーザが、サーバが提供するあるサービスを利用する場合において、他のユーザの承認や同意が必要な場合であっても、当該ユーザの前記サービスへのアクセス管理を適正に行うことができる。

【0025】なお、本発明において、前記クライアント

端末が複数ある場合、前記サービス提供管理手段は、さらに、複数の前記クライアント端末各々から送られたきた、当該クライアント端末を使用するユーザの識別情報を、当該クライアント端末の識別情報に対応付けて記憶する識別情報記憶手段と、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合に、当該承認条件によって定まるユーザの識別情報に対応付けられたクライアント端末の識別情報を、識別情報記憶手段から検索する識別情報検索手段と、前記識別情報検索手段で検出されたクライアント端末の識別情報によって特定されるクライアント端末に、前記サービス提供要求を送信したクライアント端末のユーザが、当該サービス提供要求を行った旨を通知する通知手段と、を備え、前記入力手段は、さらに、前記通知手段により通知されたサービス提供要求に応じた処理の承認を行うか否かを特定するための承認許諾情報の入力を受け付けるものであり、前記サービス提供実行手段は、前記承認条件検索手段で検出した承認条件が承認を必要とする旨を示している場合において、前記識別情報検索手段で検出された識別情報によって特定されるクライアント端末から送信された前記承認許諾情報が、前記サービス提供要求に応じた処理の承認を行う旨を示している場合にのみ、当該サービス提供要求に応じた処理を実行するものであることが好ましい。

【0026】このようにすることで、サービス提供要求に承認を与えることができるユーザが、クライアント端末を介して当該承認を行うか否かをサーバに通知することにより、前記サービス提供要求に応じた処理を行うか否かが決定される。

【0027】したがって、従来のクライアント・サーバシステムに比べ、サービス提供要求に承認が必要となる場合において、当該サービス提供要求を行ったユーザや、サーバの管理者にかかる負担を軽減することができる。

【0028】また、本発明のサーバは、クライアント端末に少なくとも1つのサービスを提供するサーバであって、前記少なくとも1つのサービス各々について、前記クライアント端末を利用する複数のユーザの識別情報、あるいは当該識別情報によって定まるユーザのレベル情報と、当該サービスの提供を受けるための承認の有無、および承認が必要な場合に当該承認を与えることができる少なくとも一人のユーザの識別情報を特定するための承認条件と、の対応関係を示す管理テーブルが記憶された管理テーブル記憶手段と、前記少なくとも1つサービスの前記クライアント端末への提供を管理するサービス提供管理手段と、を備え、前記サービス提供管理手段は、前記クライアント端末から送信された、あるサービスについてのサービス提供要求について、当該クライアント端末の識別情報、あるいは当該識別情報によって定まるユーザのレベル情報に対応付けられた承認条件を、

前記管理テーブル記憶手段から検索する承認条件検索手段と、前記承認条件検索手段で検出した承認条件が、承認を必要としない旨を示している場合は、当該サービス提供要求に応じた処理を実行し、承認を必要とする旨を示している場合は、当該承認条件によって定まるユーザの識別情報を有するユーザの承認を受けた後に、当該サービス提供要求に応じた処理を実行するサービス提供実行手段と、を備えていることを特徴とする。

【0029】また、本発明のクライアント端末は、ユーザの識別情報の入力や、サーバが提供するあるサービスについてのサービス提供要求といった、当該クライアント端末を利用しているユーザの指示を受け付ける入力手段と、前記入力手段で受け付けた前記ユーザの指示を、前記サーバに送信する送信手段とを備え、前記サーバから提供されたサービスを享受するクライアント端末であって、前記サーバから通知された、他のクライアント端末のユーザが行ったサービス提供要求に関する情報を表示する表示手段を有し、前記入力手段は、前記表示手段により表示された、他のクライアント端末のユーザが行ったサービス提供要求について、前記サーバで当該サービス提供要求に応じた処理を実行するために必要な承認の入力をも受け付けるものである、ことを特徴とする。

【0030】

【発明の実施の形態】以下に、本発明の一実施形態について、図面を参照して説明する。

【0031】図1は本発明の一実施形態が適用されたクライアント・サーバシステムの概略構成を示す図である。

【0032】本実施形態のクライアント・サーバシステムは、図1に示すように、クライアント端末1〜1_n（以下、単にクライアント端末1とも称する）と、サーバ2とが、LANなどの通信網3を介して、互いに接続されて構成されている。

【0033】サーバ2は、クライアント端末1に、様々なサービスを提供する。ここでサービスとは、たとえば、サーバ2が所有するあるオブジェクト（ファイル等）へのアクセス（読み取り、書き込み、実行等）を認めることなど、サーバ2が有する資源の活用をクライアント端末1に認めることを意味する。

【0034】ユーザは、クライアント端末1を介して、サーバ2が提供する様々なサービスを受けることができる。クライアント端末1およびサーバ2間のデータのやり取りは、通信網3を介して行われる。

【0035】なお、サーバ2には、クライアント端末1を使用するユーザを管理するためのユーザ管理ファイルや、サーバ2が提供する様々なサービスを管理するためのサービス管理ファイルなどを格納するための記憶装置4が接続されている。ユーザ管理ファイルおよびサービス管理ファイルについては後述する。

【0036】次に、本実施形態のクライアント・サーバ

システムを構成するクライアント端末1およびサーバ2のハードウェア構成について、図面を参照して説明する。

【0037】図2はクライアント端末1のハードウェア構成を示す図である。

【0038】本実施形態のクライアント端末1のハードウェア構成は、図2に示すように、通信網インタフェース11と、表示装置12と、入力装置13と、中央処理装置(CPU)14と、メモリ15とが、バス16によって互いに接続されて構成されている。

【0039】通信網インタフェース11は、通信網3を介してサーバ2とデータのやり取りを行うためのインタフェースである。

【0040】表示装置12は、クライアント端末1のユーザにメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0041】入力装置13は、クライアント端末1のユーザがデータや指令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0042】CPU14は、クライアント端末1を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0043】メモリ15には、OS(オペレーティングシステム)15aや、通信プログラム15b、あるいはサーバサービス利用プログラム15cといった、CPU14が上記の処理を実行するために必要なプログラムが格納されている。

【0044】ここで、OS15aは、クライアント端末1全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0045】通信プログラム15bは、クライアント端末1がサーバ2とデータのやり取りを行うためのプログラムである。

【0046】サーバサービス利用プログラム15cは、サーバ2が提供する各種サービスを利用する際に必要なすべての処理を制御するプログラムである。

【0047】なお、メモリ15は、ROMやRAMといった主記憶装置の他、ハードディスクやフロッピーディスク、あるいはCD-ROMなどの外部記憶装置であってもよい。

【0048】図3はサーバ2のハードウェア構成を示す図である。

【0049】本実施形態のサーバ2のハードウェア構成は、図3に示すように、通信網インタフェース21と、記憶装置インターフェース22と、表示装置23と、入力装置24と、中央処理装置(CPU)25と、メモリ26とが、バス27によって互いに接続されて構成されている。

【0050】通信網インタフェース21は、通信網3を

介してクライアント端末1とデータのやり取りを行うためのインタフェースである。

【0051】記憶装置インターフェース22は、記憶装置4とデータのやり取りを行うためのインタフェースである。

【0052】表示装置23は、システム管理者にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0053】入力装置24は、システム管理者が記憶装置4に格納したユーザ管理ファイル41やサービス管理ファイル42の内容を補充・削除したり、更新したりするために用いられるものであり、キーボードやマウスなどで構成される。

【0054】CPU25は、サーバ2を構成する各部や記憶装置4を統括的に制御したり、様々な演算処理を行ったりする。

【0055】メモリ26には、OS(オペレーティングシステム)26aや、通信プログラム26b、あるいはサーバサービス利用プログラム26c、サーバサービス制御プログラム26dといった、CPU25が上記の処理を実行するために必要なプログラムが格納されている。

【0056】ここで、OS26aは、サーバ1全体および記憶装置4の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0057】通信プログラム26bは、サーバ2がクライアント端末1とデータのやり取りを行うためのプログラムである。

【0058】サーバサービス処理プログラム26cは、クライアント端末1から送られてきた、当該クライアント端末1のユーザのサービス提供要求に応じて、当該クライアント端末1に各種サービスを提供するためのプログラムである。

【0059】サーバサービス制御プログラム26dは、CPU25がサーバサービス処理プログラム26cを実行するか否かを制御するためのプログラムである。

【0060】なお、メモリ26は、ROMやRAMといった主記憶装置の他、ハードディスクやフロッピーディスク、あるいはCD-ROMなどの外部記憶装置であってもよい。

【0061】次に、図3に示す記憶装置4に格納されているユーザ管理ファイル41およびサービス管理ファイル42について説明する。

【0062】図4はユーザ管理ファイル41に格納されている情報の一例を説明するための図である。

【0063】ユーザ管理ファイル41は、クライアント端末1を利用して、サーバ2が提供するサービスを受けることができるユーザを管理するためのファイルであり、当該ファイル41には、図4に示すように、クライ

アント端末1を利用する複数のユーザ各々について、ユーザ識別子と、パスワードと、ユーザ権限レベルとが対応付けられたテーブルが格納されている。

【0064】ここで、ユーザ識別子およびパスワードは、ユーザがクライアント端末1を介してサーバ2が提供する各種サービスを利用できる状態にするために必要なデータ、すなわち本実施形態のクライアント・サーバシステムにログインするために必要なデータである。

【0065】ユーザ権限レベルは、これに対応付けられたユーザ識別子およびパスワードを有するユーザに与えられた、当該ユーザが各種サービスを利用する場合の条件を定めるのに用いるデータである。

【0066】図5はサービス管理ファイル42に格納されている情報の一例を説明するための図である。

【0067】サービス管理ファイル42は、クライアント端末1のユーザが利用可能なサービスを管理するためのファイルであり、図5に示すように、サーバ2が提供するサービス各々について、サービス識別子と、図4に示すユーザ権限レベルと、処理制御ルールとが対応付けられたテーブルが格納されている。

【0068】ここで、サービス識別子は、クライアント端末1のユーザが提供を要求したサービスを特定するためのデータである。処理制御ルールは、これに対応付けられたサービス識別子で特定されるサービスの提供が可能であるか否か、および提供が可能である場合に、他のユーザの承認が必要であるか否かを定めるデータである。

【0069】図5に示す例では、「A」というサービス識別子で特定されるサービスは、ユーザ権限レベル「0」のユーザならば「常に利用可能」であり、ユーザ権限レベル「1」のユーザならば、「ユーザ識別子が"taro"であるユーザの承認が得られた」ときに利用可能であることを示している。また、ユーザ権限レベル「2」および「3」のユーザは、利用不可であることを示している。

【0070】なお、上記のユーザ管理ファイル41と、サービス管理ファイル42とは、機密漏洩などの不正使用防止の観点から、本実施形態のクライアント・サーバシステムの管理者のみがアクセスできるようにして、クライアント端末1のユーザはアクセスできないようにすることが好ましい。

【0071】次に、本実施形態のクライアント・サーバシステムを構成するクライアント端末1およびサーバ2の機能ブロック構成について、図面を参照して説明する。

【0072】図6はクライアント端末1およびサーバ2の機能ブロック構成を示す図である。ここで、クライアント端末1の各機能ブロックは、クライアント端末1のCPU14がメモリ15に格納された各プログラム15a~15cを実行することで実現される。また、サーバ

2の各機能ブロックは、サーバ2のCPU25がメモリ26に格納された各プログラム26b~26dを実行することで実現される。

【0073】まず、クライアント端末1の機能ブロック構成について説明する。

【0074】クライアント端末1は、図6に示すように、クライアント端末1のユーザの指示の受け付ける入力部101と、サーバ2から送信された情報を表示する表示部102と、入力部101に入力されたユーザの指示にしたがいサーバ2に対してログイン要求を行うログイン要求処理部103と、入力部101に入力されたユーザの指示にしたがいサーバ2に対して所望のサービスの提供を行うサービス提供要求処理部104と、サーバ2から提供されたサービスの享受処理を行うサービス享受処理部105と、他のユーザ（このクライアント端末1を使用しているユーザ以外のユーザ）が行ったサービス提供要求を承認するか否かの処理を行うサービス承認処理部106と、入力部101に入力されたユーザの指示にしたがいサーバ2に対してログアウト要求を行うログアウト要求処理部107と、を有する。

【0075】ログイン要求処理部103は、ユーザが入力部101に入力した、当該ユーザのユーザ識別子およびパスワードと、クライアント端末1の識別子を含むログイン要求をサーバ2に送信する。

【0076】サービス提供要求部104は、ユーザが入力部101に入力した、サーバ2が提供するあるサービスについての提供要求を、当該要求にクライアント端末1の識別子を含めて、サーバ2に送信する。

【0077】サービス承認処理部105は、サーバ2から送られてきた、他のユーザが行ったサービス提供要求を承認するか否かの判断要求である承認要求を、表示部102に表示して、ユーザに、当該他のユーザが行ったサービス提供要求を承認するか否かの判断を促す。そして、入力部101に入力された、前記承認するか否かの判断が示された承認情報を、サーバ2に送信する。

【0078】サービス享受処理部106は、サーバ2から送信されたサービス情報、あるいは当該情報によって定まる情報を表示部102に表示したりして、ユーザに提供する。

【0079】ログアウト要求処理部107は、ユーザが入力部101に入力した、ログアウト要求を、当該要求にクライアント端末1の識別子を含めて、サーバ2に送信する。

【0080】次に、サーバ2の機能ブロック構成について説明する。

【0081】サーバ2は、図6に示すように、クライアント端末1から送信されたログイン要求にしたがいログイン処理を行うログイン処理部201と、ログインしているクライアント端末1のユーザに関する情報を記憶するログイン管理テーブル202と、クライアント端末1

から送信されたログアウト要求にしたがいログアウト処理を行うログアウト処理部 203 と、クライアント端末 1 へのサービス提供を管理するサービス管理部 204 と、を有する。

【0082】ログイン処理部 201 は、クライアント端末 1 から送信されたログイン要求に含まれる当該クライアント端末 1 のユーザ識別子およびパスワードを、予め記憶装置 4 のユーザ管理ファイル 41 に記憶された、図 4 に示すようなテーブルから検索する。

【0083】そして、前記テーブルからユーザ識別子およびパスワードを検出することができた場合は、当該ユーザ識別子と、当該ユーザ識別子およびパスワードに対応付けられたユーザ権限レベルと、前記ログイン要求に含まれるクライアント端末 1 の識別子とを、ログイン管理テーブル 202 に転送する。

【0084】一方、前記テーブルからユーザ識別子およびパスワードを検出することができなかった場合は、前記ログイン要求を送信したクライアント端末 1 に、ログインできない旨を通知する。

【0085】ログイン管理テーブル 202 には、ログイン処理部 201 から送られてきた、ユーザの識別子、ユーザ権限レベルおよびクライアント端末 1 の識別子を一組とするユーザ情報のリストが格納される。

【0086】図 7 にログイン管理テーブル 202 に格納されたユーザ情報リストの一例を示す。このユーザ情報リストは、後述するサービス管理部 204 でのサービス提供の管理に用いられる。

【0087】ログアウト処理部 203 は、ログイン管理テーブル 202 に記憶されたユーザ情報リストから、クライアント端末 1 から送信されたログアウト要求に含まれる当該クライアント端末 1 の識別子と、当該識別子に対応付けられたユーザ識別子およびユーザ権限レベルとからなるユーザ情報を削除する。

【0088】サービス管理部 204 は、上述したように、クライアント端末 1 へのサービス提供を管理するものであり、サービス管理処理部 205 と、サービス承認要求処理部 206 と、サービス提供処理部 207 と、を有する。

【0089】サービス管理処理部 205 は、クライアント端末 1 から送られてきたサービス提供要求に含まれる当該クライアント端末 1 の識別子に対応付けられたユーザ権限レベルを、ログイン管理テーブル 202 から検索する。

【0090】次に、検出したユーザ権限レベルと、前記サービス提供要求によって定まるサービス識別子とに対応付けられた処理制御ルールを、予め記憶装置 4 のサービス管理ファイル 42 に記憶された、図 5 に示すようなテーブルから検索する。

【0091】そして、検出した処理制御ルールを、前記サービス提供要求に含まれる当該クライアント端末 1 の

識別子と、前記サービス提供要求で定まるサービス識別子とともに、サービス承認要求部 206 に送信する。

【0092】サービス承認要求処理部 206 は、サービス管理処理部 205 から送られてきた処理制御ルールを解析する。そして、解析結果に応じた処理を行う。

【0093】たとえば、処理制御ルールが、承認不要を意味するものである場合は、サービス管理処理部 205 から当該処理制御ルールとともに送られてきたクライアント端末 1 の識別子とサービス識別子とを、サービス提供処理部 207 に転送して、当該サービス識別子で定まる内容のサービスを、当該クライアント端末 1 の識別子で特定されるクライアント端末 1 に提供するように指示する。

【0094】また、処理制御ルールが、あるユーザの承認が必要であることを意味する場合は、当該ユーザが使用するクライアント端末 1 に対して、前記サービス提供要求を送信したクライアント端末 1 のユーザが、当該サービス提供要求によって定まるサービスを享受することについて、承認するか否かの判断を要求する承認要求を送信する。

【0095】そして、承認要求の送信先のクライアント端末 1 から、承認する旨の承認情報が送られてきた場合は、サービス管理処理部 205 から当該処理制御ルールとともに送られてきたクライアント端末 1 の識別子とサービス識別子とを、サービス提供処理部 207 に転送して、当該サービス識別子で定まる内容のサービスを、当該クライアント端末 1 の識別子で特定されるクライアント端末 1 に提供するように指示する。

【0096】一方、承認要求の送信先のクライアント端末 1 から、承認しない旨の承認情報が送られてきた場合は、サービス管理処理部 205 から当該処理制御ルールとともに送られてきたクライアント端末 1 の識別子で特定されるクライアント端末 1 に、サービス提供の承認が拒否された旨を通知する。

【0097】また、処理制御ルールが、サービスの提供拒否を意味する場合は、サービス管理処理部 205 から当該処理制御ルールとともに送られてきたクライアント端末 1 の識別子で特定されるクライアント端末 1 に対して、同じく当該処理制御ルールとともに送られてきたサービス識別子で定まる内容のサービス提供が拒否された旨を通知する。

【0098】サービス提供処理部 207 は、サービス承認要求処理部 206 から送られてきたサービス識別子で定まる内容のサービスを実行する。そして、実行結果などを当該サービス識別子とともに送られてきたクライアント端末 1 の識別子で特定されるクライアント端末 1 に提供する。

【0099】次に、本実施形態のクライアント・サーバシステムの動作について説明する。

【0100】まず、ユーザがサーバ 2 にサービス提供を

10

20

30

40

50

要求する場合におけるクライアント端末1の動作について説明する。

【0101】図8は、ユーザがサーバ2にサービス提供を要求する場合におけるクライアント端末1の動作を説明するためのフロー図である。

【0102】まず、ユーザが入力部101に、当該ユーザのユーザ識別子およびパスワードを入力すると（ステップ1001）、ログイン要求処理部103は、このユーザ識別子およびパスワードと、自己のクライアント端末1の識別子とを含むログイン要求をサーバ2に送信する（ステップ1002）。

【0103】次に、ログイン要求処理部103は、サーバ2から送られてきたログインを許可するか否かを示すログイン情報を受け取り、このログイン情報がログインを許可する旨を示している場合は、その旨を表示部102に表示した後（ステップ1005）、ステップ1006に移行する（ステップ1003）。

【0104】一方、ログイン情報がログインを許可しない旨を示している場合は、その旨を表示部102に表示した後（ステップ1004）、このフローを終了する。この場合、クライアント端末1のユーザは、サーバ2が提供する各種サービスを受けることができない。

【0105】ステップ1006では、ユーザが入力部1041に、サーバ2が提供するあるサービスの提供を要求する旨の指示を入力すると、サービス提供要求処理部104は、当該サービスの提供要求に、自己のクライアント端末1の識別子を含めて、サーバ2に送信する（ステップ1007）。

【0106】たとえば、ユーザが、サーバ2が有するあるファイルに対する読み込み要求を行うと、当該要求が自己のクライアント端末1の識別子とともに、サーバ2に送信される。

【0107】なお、ステップ1006において、サービス提供の要求が入力されていない場合は、ステップ1012に移行する。

【0108】次に、クライアント端末1は、サーバ2から送られてきた情報に応じた処理を行う（ステップ1008）。

【0109】具体的には、サーバ2から送られてきた情報が、ステップ1007で送信したサービス提供要求を許可しない旨を示している場合、サービス提供要求処理部104は、その旨を表示部102に表示し（ステップ1009）、その後、ステップ1012に移行する。

【0110】また、サーバ2から送られてきた情報が、ステップ1007で送信したサービス提供要求を許可するための承認が得られなかった旨を示している場合、その旨を表示して（ステップ1010）、ステップ1012に移行する。

【0111】図14は、サービス提供要求を許可するための承認が得られなかった場合に、当該サービス提供要

求を行ったクライアント端末1の表示部102に表示される画面の一例を示している。

【0112】また、サーバ2から送られてきた情報が、ステップ1007で送信したサービス提供要求に応じて提供されたサービス情報である場合、このサービス情報、あるいはこのサービス情報によって定まる情報を、表示部102に表示したりして、ユーザに提供し（ステップ1011）、その後、ステップ1012に移行する（ステップ1009）。

【0113】その後、ユーザが入力部101にログアウト要求を入力すると（ステップ1012）、ログアウト要求処理部107は、自己のクライアント端末1の識別子を含むログアウト要求をサーバ2に送信し（ステップ1013）、このフローを終了する。一方、ログアウト要求が入力されていない場合は、ステップ1006に戻る。

【0114】次に、ユーザが、他のユーザが行ったサービス提供要求を承認するか否かを決定する場合における、クライアント端末1の動作について説明する。

【0115】図9は、ユーザが、他のユーザが行ったサービス提供要求を承認するか否かを決定する場合における、クライアント端末1の動作を説明するためのフロー図である。

【0116】ステップ2001～2005は、クライアント端末1がログインするために要求される処理であり、図8に示すフローのステップ1001～1005に相当する。したがって、ログインに失敗した場合は、クライアント端末1のユーザは、他のクライアント端末1を使用するユーザが行ったサービス提供要求に承認を与えることができない。

【0117】ステップ2006では、サービス承認処理部105は、他のクライアント端末1を使用するユーザが行ったサービス提供要求についての承認要求が、サーバ2から送られてきたか否かを判断する。承認要求が送られてきた場合はステップ2007に移行し、送られてきていない場合は、ステップ2011に移行する。

【0118】ステップ2007では、承認要求があった旨を表示部102に表示して、当該承認要求によって特定される他のユーザが行ったサービス提供供給を承認するか否かの判断を促す。

【0119】図15は、承認要求があった場合に表示部102に表示される画面の一例を示す図である。この例では、サービス提供要求を行ったユーザの識別子、ユーザ権限レベル、およびサービス提供要求の対象となるサービスの識別子を表示して、承認要求を認めるか否かを選択ボタンを選択させるようにしている。

【0120】次に、サービス承認要求処理部105は、ステップ2007で表示した承認要求について、ユーザが、当該承認要求を承諾する旨を選択したか否かを判断する（ステップ2008）。

【0121】ユーザが当該承認要求を許諾する旨選択している場合は、当該承認要求について許諾した旨を示す承認許諾情報を、自己のクライアント端末1の識別子とともに、サーバ2に送信する(ステップ2009)。

【0122】一方、ユーザが当該承認要求を拒否する旨選択している場合は、当該承認要求について拒否した旨を示す承認拒否情報を、自己のクライアント端末1の識別子とともに、サーバ2に送信する(ステップ2010)。

【0123】その後、ユーザが入力部101にログアウト要求を入力すると(ステップ2011)、ログアウト要求処理部107は、自己のクライアント端末1の識別子を含むログアウト要求をサーバ2に送信し(ステップ2012)、このフローを終了する。一方、ログアウト要求が入力されていない場合は、ステップ2006に戻る。

【0124】次に、サーバ2の動作について説明する。

【0125】図10および図11はサーバ2の動作を説明するためのフロー図である。

【0126】まず、図10に示すフローにおいて、ログイン処理部201は、クライアント端末1からログイン要求が送信されたか否かを判断する(ステップ3001)。ログイン要求が送られてきた場合はステップ3002に移行し、送られてきていない場合はステップ3005に移行する。

【0127】ステップ3002では、ログイン処理部201は、ステップ3001で受信したログイン要求に含まれるクライアント端末1のユーザ識別子およびパスワードを、予め記憶装置4のユーザ管理ファイル41に記憶されたテーブルから検索する。

【0128】そして、前記テーブルからこのユーザ識別子およびパスワードを検出することができた場合は、当該ユーザ識別子と、当該ユーザ識別子およびパスワードに対応付けられたユーザ権限レベルと、前記ログイン要求に含まれるクライアント端末1の識別子とを、ログイン管理テーブル202に転送し、格納する(ステップ3003)。

【0129】たとえば、ユーザ管理ファイル41に記憶されているテーブルが図4に示すものであり、ステップ3001で受信したログイン要求に含まれるクライアント端末1のユーザ識別子が「taro」、パスワードが「12345678」、そしてクライアント端末1の識別子が「12」であるとする。

【0130】この場合、ログイン処理部201は、ユーザ識別子が「taro」と、ユーザ権限レベル「0」と、クライアント端末1の識別子「12」とを、ログイン管理テーブル202に転送し、格納することになる。

【0131】一方、前記テーブルからこのユーザ識別子およびパスワードを検出することができなかった場合は、前記ログイン要求を送信したクライアント端末1

に、ログインできない旨を通知する(ステップ3004)。

【0132】ステップ3005では、サービス管理処理部205は、クライアント端末1からサービス提供要求が送信されたか否かを判断する。サービス提供要求が送られてきた場合はステップ3006に移行し、送られてきていない場合は図11に示すフローのステップ3020に移行する。

【0133】ステップ3006では、サービス管理処理部205は、ステップ3005で受信したサービス提供要求に含まれるクライアント端末1の識別子に対応付けられたユーザ権限レベルを、ログイン管理テーブル202から検索する。

【0134】そして、検出したユーザ権限レベルと、前記サービス提供要求によって定まるサービス識別子とに対応付けられた処理制御ルールを、予め記憶装置4のサービス管理ファイル42に記憶されたテーブルから検索する(ステップ3007)。たとえば、ログイン管理テーブル202に記憶されているテーブルが図7に示すものであり、且つサービス管理ファイル42に記憶されているテーブルが図5に示すものであり、加えて、ステップ3005で受信したサービス提供要求に含まれるクライアント端末1の識別子が「11」、当該サービス提供要求によって定まるサービス識別子が「A」とであるとする。

【0135】この場合、サービス管理処理部205は、まず、クライアント端末1の識別子「11」に対応付けられたユーザ権限レベル「1」およびユーザ識別子「jirro」を、図7に示すテーブルから検出することになる。次に、検出したユーザ権限レベル「1」と、サービス識別子「A」とに対応付けられた処理制御ルール「"tar o"の承認が必要」を、図5に示すテーブルから検出することになる。

【0136】次に、サービス管理処理部205は、ステップ3007で検出した処理制御ルールを、ステップ3005で受信したサービス提供要求に含まれるクライアント端末1の識別子と、このサービス提供要求で定まるサービス識別子とともに、サービス承認要求部206に送信する(ステップ3008)。

【0137】その後、図11に示すフローのステップ3009に移行する。

【0138】ステップ3009では、サービス承認要求処理部206は、ステップ3008において、サービス管理処理部205から送られてきた処理制御ルールを解析する。そして、解析結果に応じた処理を行う。

【0139】具体的には、解析した処理制御ルールが、当該処理制御ルールに対応付けられたサービス提供についての承認不要を意味するものである場合は、ステップ3008でサービス管理処理部205から送られてきたクライアント端末1の識別子とサービス識別子とを、サ

ービス提供処理部 207 に転送する（ステップ 3010）。

【0140】たとえば、ステップ 3008 でサービス管理処理部 205 から送られてきたクライアント端末 1 の識別子が「1₂」、サービス識別子が「A」、処理制御ルールが「常に処理可能」である場合、サービス承認要求処理部 206 は、サービス識別子「A」およびクライアント端末 1 の識別子「1₂」を、サービス提供処理部 207 に転送する。

【0141】また、解析した処理制御ルールが、当該処理制御ルールに対応付けられたサービスについての提供拒否を意味する場合は、ステップ 308 でサービス管理処理部 205 から送られてきたクライアント端末 1 の識別子で特定されるクライアント端末 1 に、サービス提供が拒否された旨を通知し（ステップ 3011）、その後、ステップ 3020 に移行する。

【0142】たとえば、ステップ 3008 でサービス管理処理部 205 から送られてきたクライアント端末 1 の識別子が「1₃」、サービス識別子が「A」、処理制御ルールが「処理不可能」である場合、サービス承認要求処理部 206 は、クライアント端末 1 の識別子「1₃」で定まるクライアント端末 1 に、サービス識別子「A」で定まるサービス提供が拒否された旨を通知する。

【0143】さらに、解析した処理制御ルールが、当該処理制御ルールに対応付けられたサービスの提供を受けるために、あるユーザの承認が必要であることを意味する場合は、当該ユーザが使用するクライアント端末 1 の識別子をログイン管理テーブル 202 に記憶されたテーブルから検索し（ステップ 3012）、その後、ステップ 3013 に移行する。

【0144】たとえば、ログイン管理テーブル 202 に記憶されたテーブルが図 7 に示すものであるとする。

【0145】ここで、ステップ 3008 でサービス管理処理部 205 から送られてきたクライアント端末 1 の識別子が「1₁」、サービス識別子が「C」、そして処理制御ルールが「レベル 0 の承認が△人必要」である場合、ユーザ権限レベル「0」に対応付けられたクライアント端末 1 の全てを、図 7 に示すテーブルから検出することになる。

【0146】また、ステップ 3008 でサービス管理処理部 205 から送られてきたクライアント端末 1 の識別子が「1₁」、サービス識別子が「A」、そして処理制御ルールが「"taro" の承認が必要」である場合、ユーザ識別子「taro」に対応付けられたクライアント端末「1₂」を、図 7 に示すテーブルから検出することになる。

【0147】ステップ 3013 では、サービス承認要求処理部 206 は、ステップ 3012 で必要数分のクライアント端末 1 が検出できたか否かを判断する。

【0148】たとえば、ログイン管理テーブル 202 に

記憶されたテーブルが図 7 に示すものである場合、ステップ 3008 でサービス管理処理部 205 から送られてきた処理制御ルールが「レベル 0 の承認が△人必要」であるときには、ユーザ権限レベル「0」に対応付けられたクライアント端末 1 が△数以上検出できたか否かを判断する。また、ステップ 3008 でサービス管理処理部 205 から送られてきた処理制御ルールが「"taro" の承認が必要」であるときには、ユーザ識別子「taro」に対応付けられたクライアント端末 1 が検出できたか否かを判断する。

【0149】そして、必要数分のクライアント端末が検出できなかった場合は、ステップ 3005 でサービス提供要求を送信したクライアント端末 1 に、当該サービス提供要求の承認を得るために必要なユーザがログインしていない旨を通知し（ステップ 3014）、その後、ステップ 3020 に移行する。

【0150】一方、必要数分のクライアント端末が検出できた場合は、当該検出したクライアント端末 1 に、ステップ 3005 でサービス提供要求を送信したユーザが、当該サービス提供要求で特定されるサービスを享受することについて、承認するか否かの判断を要求する（ステップ 3015）。

【0151】その後、承認要求を行ったクライアント端末 1 から返答（承認情報）がくるのを待つ（ステップ 3016）。

【0152】次に、サービス承認要求処理部 206 は、処理制御ルールに示されたユーザ、あるいは処理制御ルールに示された人数分のユーザから、承認承諾情報を得られたか否かを判断する（ステップ 3017）。得られている場合はステップ 3010 に移行する。一方、得られていない場合は、その旨をステップ 3005 でサービス提供要求を送信したクライアント端末 1 に通知し（ステップ 3018）、その後、ステップ 3020 に移行する。

【0153】ステップ 3010 での処理実行後、ステップ 3011 では、サービス提供処理部 207 は、ステップ 3010 において、サービス承認要求部 206 から送られてきたサービス識別子で特定されるサービスを実行し、同じくサービス承認要求部 206 から送られてきたクライアント端末 1 の識別子で特定されるクライアント端末 1 に提供する。その後、ステップ 3020 に移行する。

【0154】ステップ 3020 では、ログアウト処理部 203 は、クライアント端末 1 からログアウト要求が送信されたか否かを判断する。ログアウト要求が送られてきた場合はステップ 3021 に移行し、送られてきていない場合はステップ 3001 に戻る。

【0155】ステップ 3021 では、ログアウト処理部 203 は、ステップ 3020 で受信したログアウト要求に含まれるクライアント端末 1 の識別子、およびこの識

10

20

30

40

50

別子に対応付けられているユーザ識別子およびユーザ権限レベルを、ログイン管理テーブル202から削除する。その後、ステップ3001に戻る。

【0156】上記の本実施形態では、クライアント端末11~1nを使用する複数のユーザ各々に、当該ユーザのユーザ権限レベルを対応付けたテーブルをユーザ管理ファイル41に格納している。また、サーバ2が提供するサービス各々について、クライアント端末1を利用する複数のユーザのユーザ権限レベルと、当該サービスの提供を受けるに際しての処理制御ルールとの対応関係を示すテーブルをサービス管理ファイル42に格納している。

【0157】そして、あるクライアント端末1から、サーバ2が提供するあるサービスに対するサービス提供要求があった場合、当該クライアント端末1を使用しているユーザに対応付けられたユーザ権限レベルを、ユーザ管理ファイル41から検索した後、前記サービスについて、当該検索したユーザ権限レベルに対応付けられた処理制御ルールを検索している。

【0158】その後、検出した処理制御ルールが、前記サービス提供要求に応じた処理を行うのに承認が必要であることを示している場合は、当該処理制御ルールによって定まるユーザの承認を受領を条件として、当該サービス提供要求に応じた処理の実行を行うようにしている。

【0159】したがって、本発明によれば、クライアント端末1のあるユーザが、サーバ2が提供するあるサービスを利用する場合において、他のユーザの承認や同意が必要な場合であっても、当該ユーザの前記サービスへのアクセス管理を適正に行うことができる。

【0160】たとえば、ユーザ権限レベルを、会社などの組織における地位に応じて付与することで、あるユーザが、サーバ2が提供するあるサービスを利用しようとする場合において、当該ユーザの上司の承認が必要な場合でも、当該サービスへのアクセス管理を適正に行うことができる。

【0161】なお、本発明は、上記の本実施形態に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【0162】たとえば、本実施形態では、ユーザにユーザ識別子およびパスワードを入力させることで、ログイン処理を行っているが、本発明はこれに限定されない。パスワードの代わりに、指紋などの生物学的特徴を用いてログイン処理を行うようにしてもよい。

【0163】すなわち、ユーザ管理ファイル41にユーザ識別子と、指紋などの生物学的特徴とを対応付けたテーブルを予め格納しておき、クライアント端末1から送られてきた、ユーザ識別子および指紋などの生物学的特徴が互いに対応付けられていることを、前記テーブルで確認することで、ログイン処理を行うようにしてもよい。

い。なお、指紋などの生物学的特徴は、たとえばスキャナなどで読み取ることができる。

【0164】また、たとえば、クライアント端末1とサーバ2との間で予め何らかの変換プログラム（たとえば暗号プログラムや一方方向性ハッシュプログラムなど）を共有させておき、パスワードを該変換プログラムで変換した結果をユーザ管理ファイル41に予め記憶させ、この変換結果を用いてログイン処理を行うようにしてもよい。

【0165】また、本実施形態において、サービス管理部205で検出された処理制御ルールが、あるユーザ権限レベルを有するユーザの承認が必要であることを意味している場合、サービス承認要求処理部206は、ログイン管理データ202に記憶されている、すなわちログインしている当該ユーザ権限レベルを有するユーザ全てに対して、当該ユーザが使用するクライアント端末1に承認要求を行っているが、このような場合、ログインしている当該ユーザ権限レベルを有するユーザの中から、サービス提供を行うのに必要とされる承認の数だけユーザを選択し、この選択したユーザに対してのみ承認要求を行うようにしてもよい。

【0166】あるいは、ログインしている当該ユーザ権限レベルを有するユーザについての一覧を、サービス提供要求を行っているクライアント端末1のユーザに提示し、承認を依頼するユーザを選択させ、選択されたユーザに対してのみ承認要求を行うようにしてもよい。

【0167】図16は、サービス提供要求を行っているクライアント端末1のユーザに、当該サービス提供要求の承認を依頼するユーザを選択させる場合に、表示部102に表示される画面の一例を示している。

【0168】ここでは、ログインしているユーザであって、サービス提供要求に承認を与えることができるユーザ権限レベルを有するユーザ各々の識別子を表示するとともに、サービス提供を受けるために必要な承認数（ここでは、一人の承認）を表示し、表示したユーザの識別子の中から、前記承認数だけ、ユーザ識別子を選択させるようにしている。

【0169】さらに、本実施形態では、サービス管理部205で検出された処理制御ルールが、あるユーザ権限レベルを有するユーザの承認が必要であることを意味している場合において、当該ユーザ権限レベルを有するユーザがログインしていない場合は、このユーザに対しては承認要求を行わないようにしている。すなわち、当該ユーザ権限レベルを有するユーザへの承認要求は、ログインしているユーザに対してのみ、リアルタイム型通信で行っている。

【0170】しかしながら、本発明はこれに限定されるものではなく、たとえば電子メールのような蓄積型通信を用いることで、ログインしていないユーザに対しても、その後ログインしたときに、承認要求を行えるようにし

てもよい。

【0171】図12は本実施形態の変形例を説明するための機能ブロック図である。図12に示すクライアント・サーバシステムが、図6に示す本実施形態のクライアント・サーバシステムと異なる点は、サーバ2aに、サービス承認要求処理部206に代えてサービス承認要求処理部206aを設けたこと、および承認要求一時記憶部210を追加したことである。

【0172】サービス承認要求処理部206aは、サービス管理処理部205から送られてきた処理制御ルールが、あるユーザの承認が必要であることを意味する場合に、ログイン管理テーブル202を参照して、当該ユーザが使用するクライアント端末1に、承認要求を送信する。当該ユーザの識別子がログイン管理テーブル202に記憶されていない場合、すなわち、当該ユーザがログインしていない場合は、当該ユーザに対する承認要求をサービス承認要求一時記憶部210に退避させる。

【0173】そして、当該ユーザの識別子がログイン管理テーブル202に記憶されたとき、すなわち、当該ユーザがログインしたときに、サービス承認要求一時記憶部210に退避させた当該ユーザに対する承認要求を、ログイン管理テーブル2020で当該ユーザの識別子に対応付けられたクライアント端末1に送信する。

【0174】その他の動作は、図6に示すサービス承認要求処理部206と同じである。

【0175】このようにすることで、ログインしていないユーザに対しても、後にログインしたときに承認要求を送信することが可能になる。

【0176】さらに、本実施形態では、サービスの提供と、サービス管理とを1台のサーバで行っているが、図13に示す本実施形態の変形例のように、各々異なるサーバで行うようにしてもよい。また、サービスを提供するサーバが複数ある場合、それら複数のサーバのサービス制御処理を1台のサーバで行うようにすれば、ユーザ管理ファイルやサービス管理ファイルが一元化できるので、システム管理者の手間をさらに軽減することができる。

【0177】くわえて、本実施形態では、サーバ2が提供するサービスを受けることができるユーザを管理するためのテーブルと、クライアント端末1のユーザが利用可能なサービスを管理するためのテーブルとを、それぞれ別個のテーブルとして、ユーザ管理ファイル41、サービス管理ファイル42に格納している。しかしながら、本発明はこれに限定されるものではなく、これ等のテーブルを一体にして記憶手段に格納するようにしてもよい。

【0178】

【発明の効果】以上説明したように、本発明によれば、クライアント端末利用者であるユーザが、サーバが提供するあるサービスを利用する場合において、他のユーザ

の承認や同意が必要な場合であっても、当該ユーザの前記サービスへのアクセス管理を適正に行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態が適用されたクライアント・サーバシステムの概略構成を示す図である。

【図2】図1に示すクライアント端末のハードウェア構成を示す図である。

【図3】図1に示すサーバのハードウェア構成を示す図である。

【図4】図3に示すユーザ管理ファイルに格納されている情報の一例を説明するための図である。

【図5】図3に示すサービス管理ファイルに格納されている情報の一例を説明するための図である。

【図6】図1に示すクライアント・サーバシステムの機能ブロック構成を示す図である。

【図7】図6に示すログイン管理テーブルに格納されたユーザ情報リストの一例を示す図である。

【図8】ユーザがサーバにサービス提供を要求する場合における、図6に示すクライアント端末の動作を説明するためのフロー図である。

【図9】ユーザが、他のユーザが行ったサービス提供要求を承認するか否かを決定する場合における、図6に示すクライアント端末の動作を説明するためのフロー図である。

【図10】図6に示すサーバの動作を説明するためのフロー図である。

【図11】図6に示すサーバの動作を説明するためのフロー図である。

【図12】本発明の一実施形態の変形例を説明するための機能ブロック図である。

【図13】本発明の一実施形態の変形例を説明するための機能ブロック図である。

【図14】サービス提供要求を許可するための承認が得られなかった場合に、当該サービス提供要求を行ったクライアント端末の表示部に表示される画面の一例を示す図である。

【図15】承認要求があった場合に、クライアント端末の表示部に表示される画面の一例を示す図である。

【図16】サービス提供要求を行っているユーザに、当該サービス提供要求の承認を依頼するユーザを選択させる場合に、クライアント端末の表示部に表示される画面の一例を示す図である。

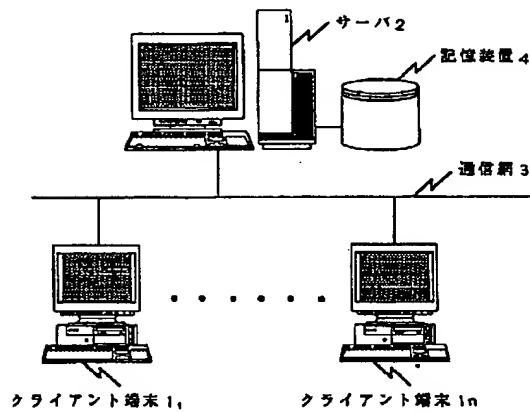
【符号の説明】

- 1 クライアント端末
- 2 2a～2c サーバ
- 3 通信網
- 4 記憶装置
- 11、21 通信網インターフェース
- 12、23 表示装置

- 13、24 入力装置
- 14、25 CPU
- 15、26 メモリ
- 15a、26a オペレーティング・システム
- 15b、26b 通信プログラム
- 15c サーバサービス利用プログラム
- 22 記憶装置インターフェース
- 26c サーバサービス処理プログラム
- 26d サーバサービス制御プログラム
- 41 ユーザ管理ファイル
- 42 サービス管理ファイル
- 101 入力部
- 102 表示部

【図1】

図1



【図4】

図4

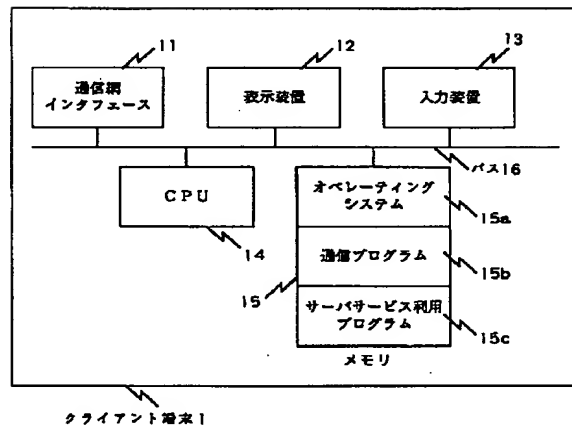
ユーザ管理ファイル

ユーザ識別子	パスワード	ユーザ権限レベル
taro	12345678	0
hanako	*****	2
sanburo	*****	2
jiro	*****	1
⋮	⋮	⋮

- 103 ログイン要求処理部
- 104 サービス提供要求処理部
- 105 サービス承認処理部
- 106 サービス享受処理部
- 107 ログアウト要求処理部
- 201 ログイン処理部
- 202 ログイン管理テーブル
- 203 ログアウト処理部
- 204 サービス管理部
- 10 205 サービス管理処理部
- 206、206a サービス承認要求処理部
- 207 サービス提供処理部
- 210 サービス承認要求一時記憶部

【図2】

図2



【図5】

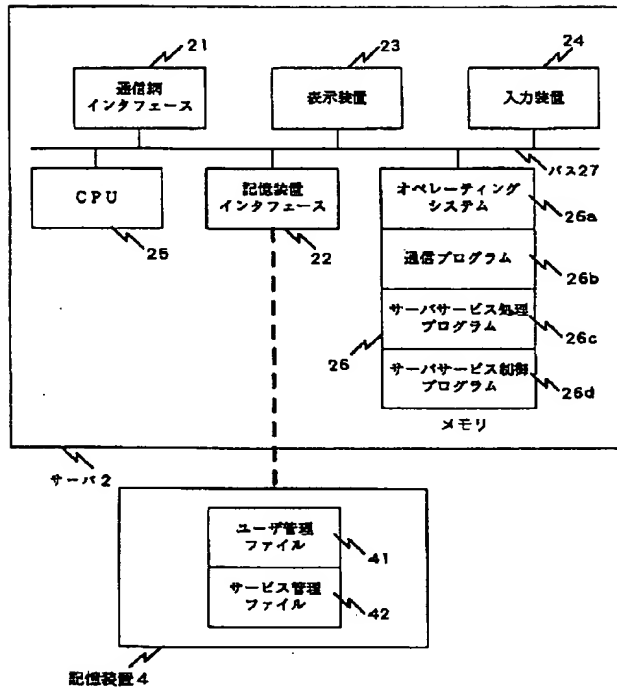
図5

サービス管理ファイル

サービス識別子	ユーザ権限レベル	処理制御ルール
A	0	常に処理可能
	1	"taro"の承認が必要
	2	処理不可
	3	処理不可
	⋮	⋮
B	0	常に処理可能
	1	常に処理可能
	2	常に処理可能
	3	常に処理可能
	⋮	⋮
C	0	常に処理可能
	1	レベル0の承認が1人必要
	2	レベル0の承認が2人必要
	3	処理不可
	⋮	⋮
⋮	⋮	⋮

【図3】

図3



【図7】

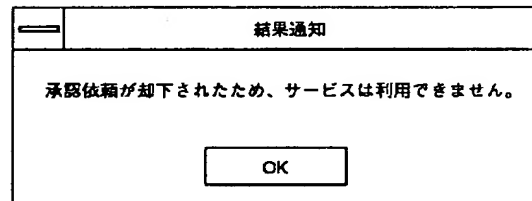
図7

ログイン管理テーブル

ユーザ識別子	ユーザ権限レベル	クライアント端末名
taro	0	クライアント端末1 _a
jiro	1	クライアント端末1 _b
⋮	⋮	⋮

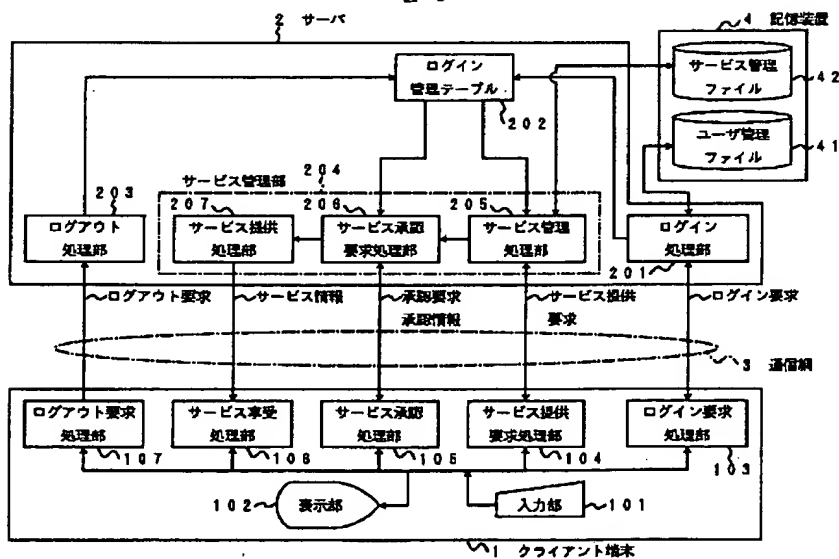
【図14】

図14



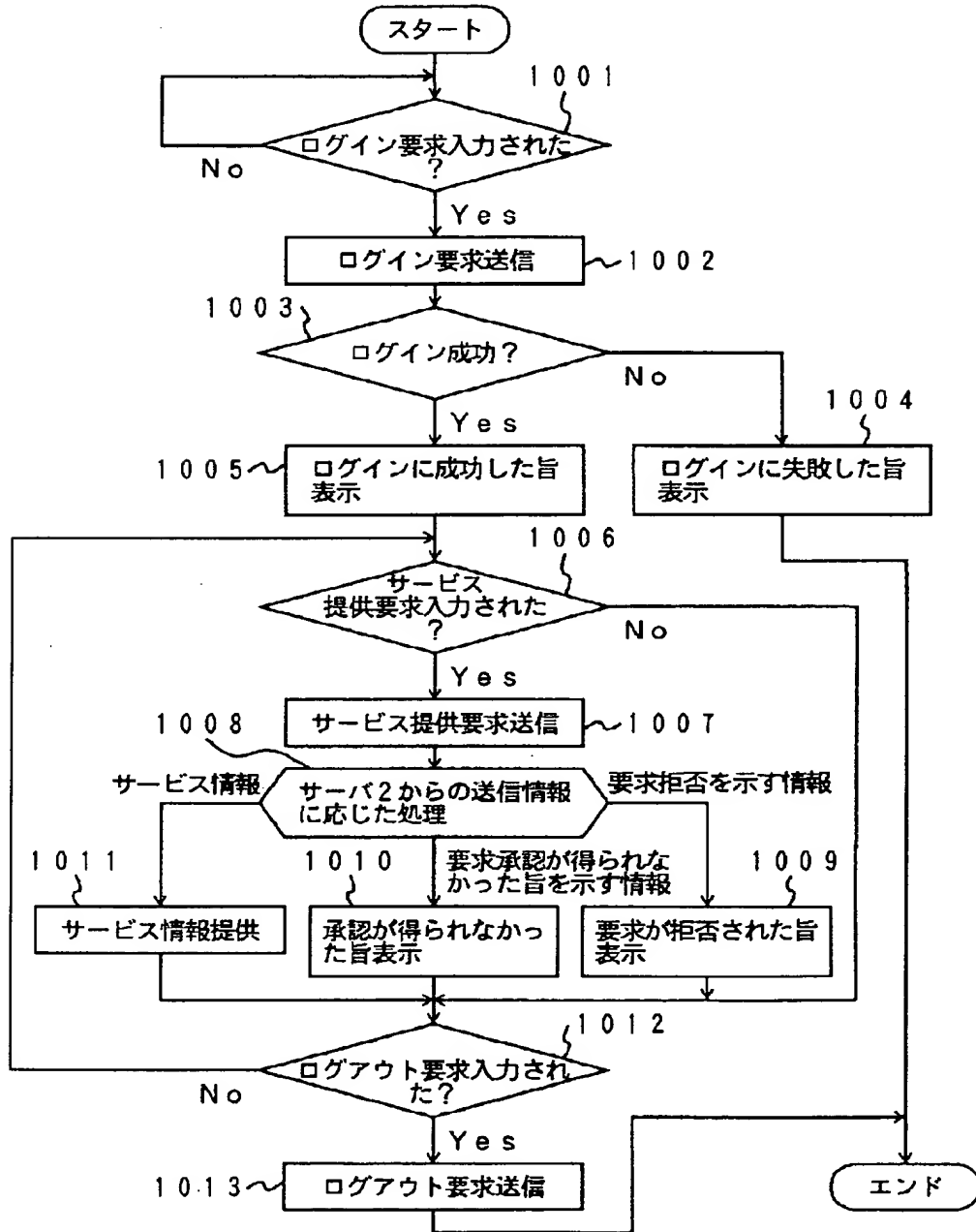
【図6】

図6



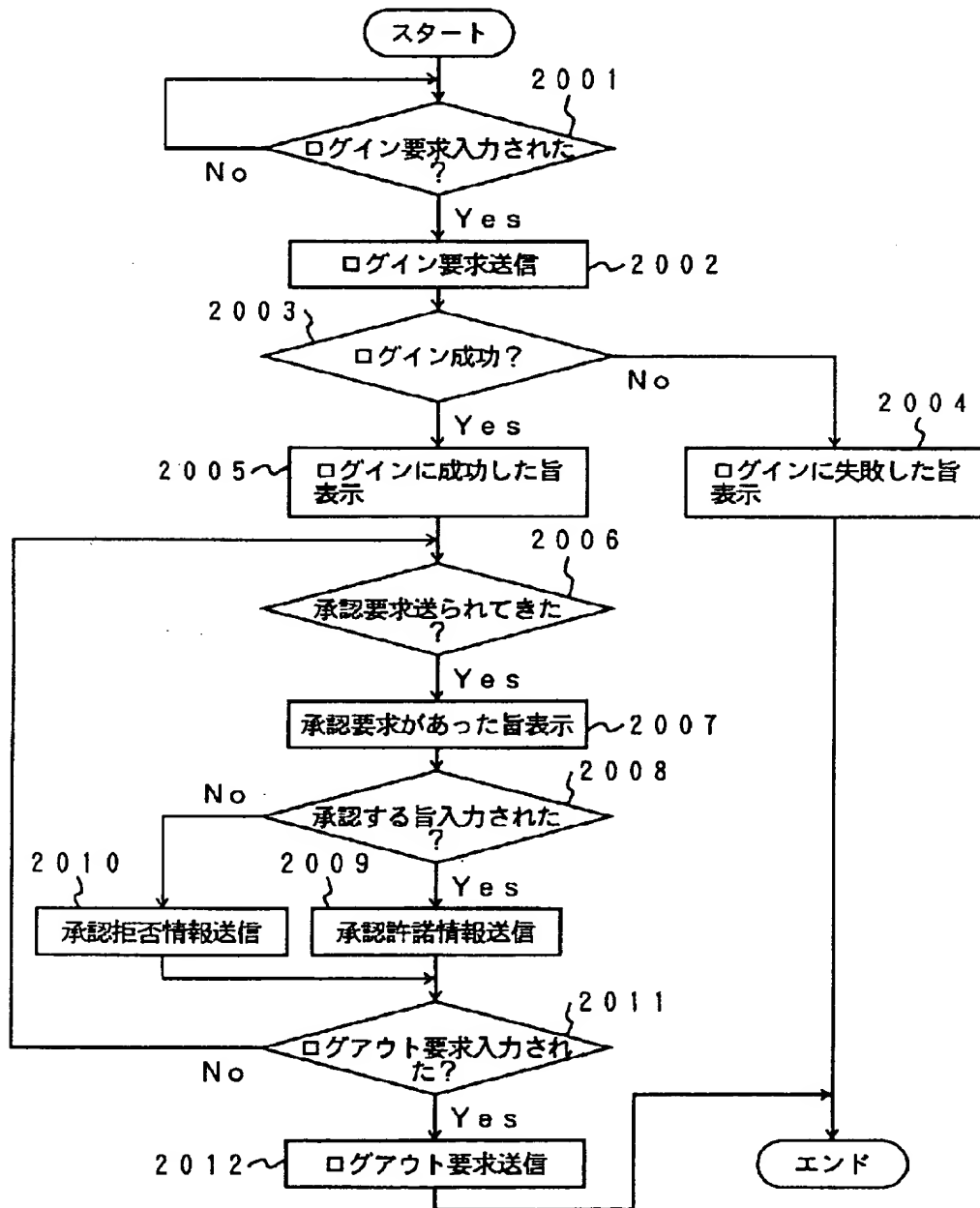
【図8】

サービス提供を要求するユーザが使用するクライアント端末1 (図8)



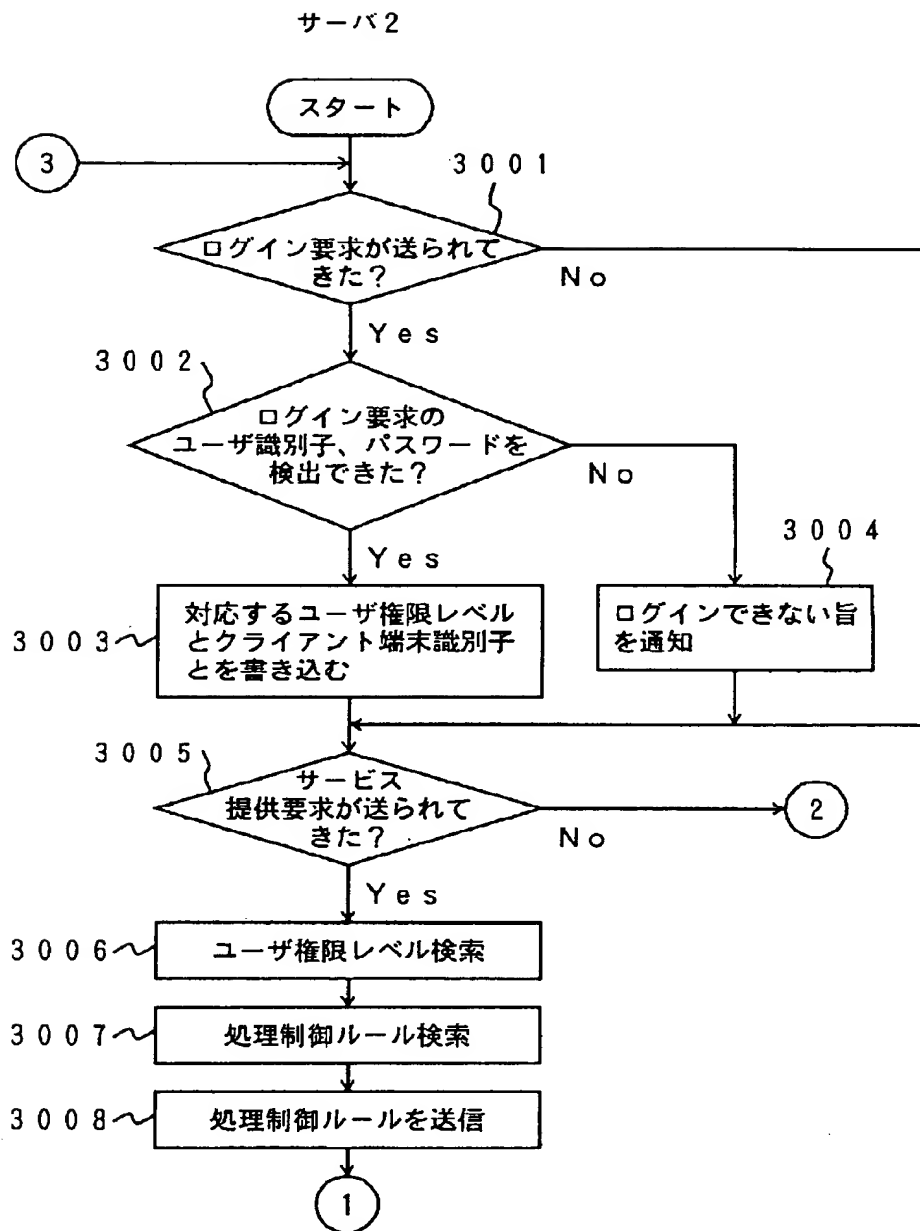
【図9】

サービス提供要求を承認するユーザが使用するクライアント端末1 (図9)



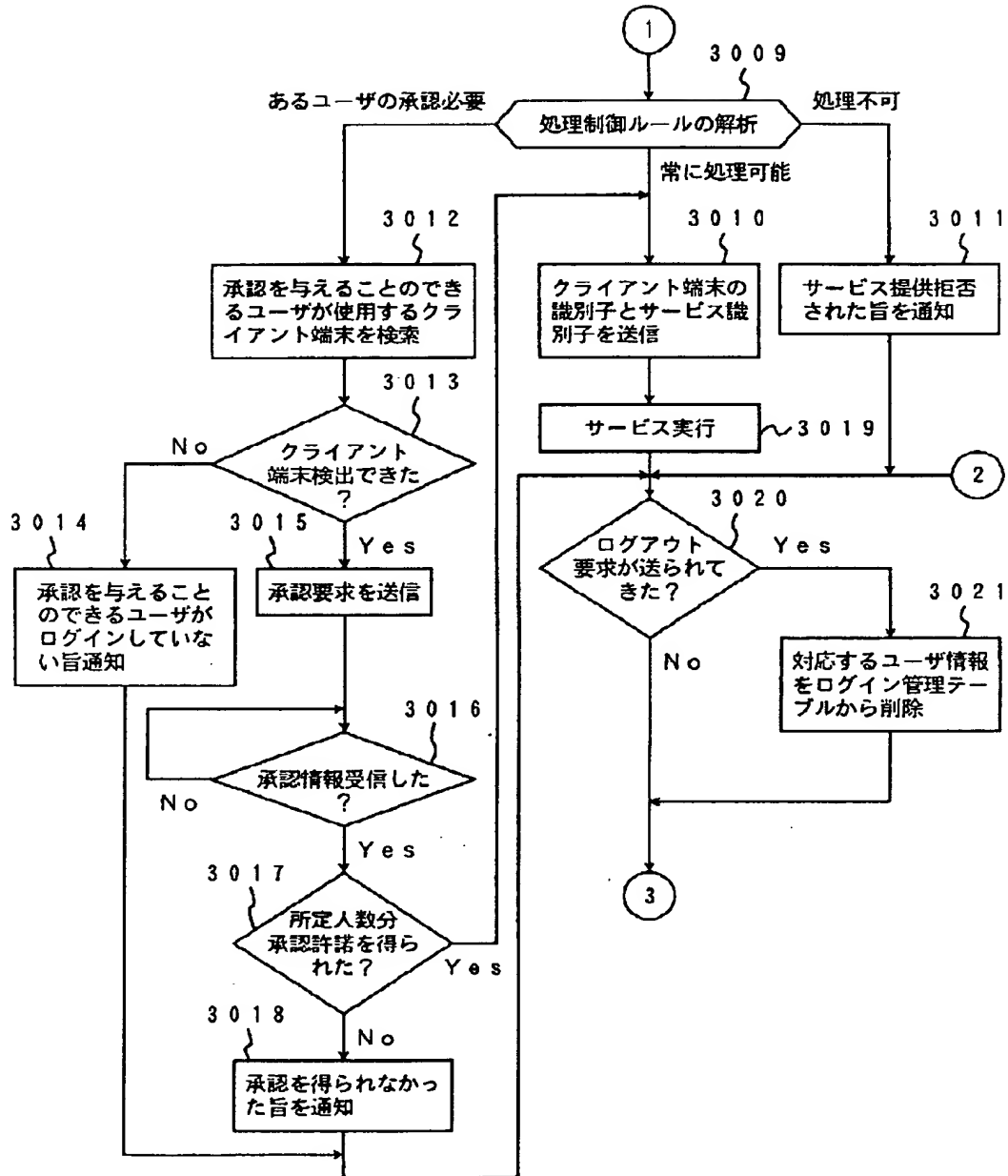
【図10】

図10

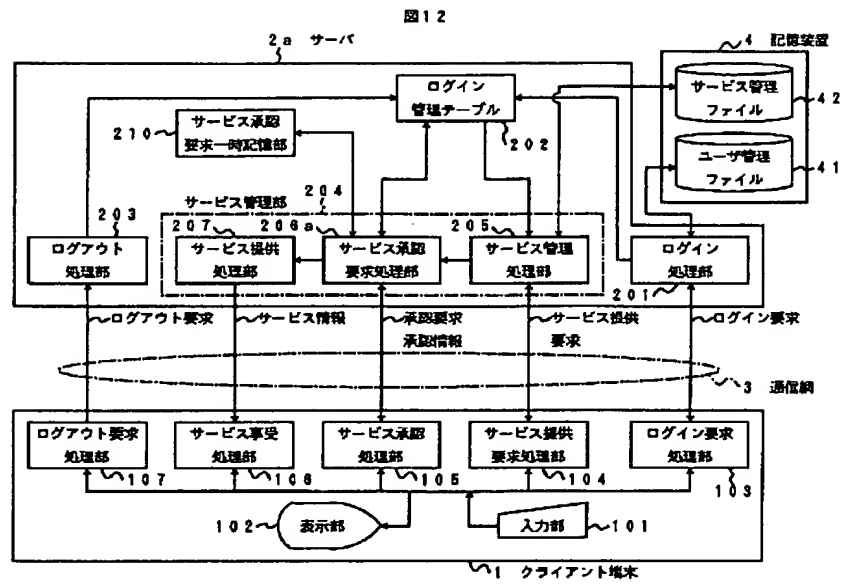


【図11】

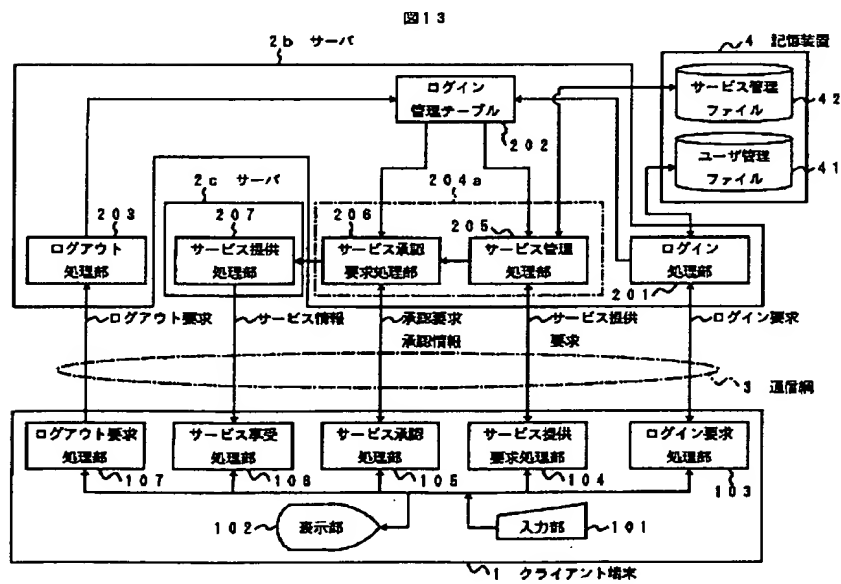
図11



【図12】



【図13】



【図15】

図 15

承認依頼の受信	
ユーザ識別子：Hanako ユーザレベル：3 サービス識別子：12	
上記の承認依頼を受信しました。承認しますか？	
承認する	却下する

【図16】

図 16

ユーザの選択									
あなたが指定したサービスを利用するためには、以下のユーザの中の1人の承認が必要です。 ユーザを選択してください。									
<table border="1"> <thead> <tr> <th>ユーザ識別子</th> <th>ユーザレベル</th> </tr> </thead> <tbody> <tr> <td>Jiro</td> <td>2</td> </tr> <tr> <td>Goro</td> <td>2</td> </tr> <tr> <td>Rokuro</td> <td>2</td> </tr> </tbody> </table>		ユーザ識別子	ユーザレベル	Jiro	2	Goro	2	Rokuro	2
ユーザ識別子	ユーザレベル								
Jiro	2								
Goro	2								
Rokuro	2								
<div>OK</div> <div>キャンセル</div>									

フロントページの続き

(72)発明者 宮▲崎▼ 誠治
 東京都小平市上水本町五丁目20番1号 株式会社日立製作所半導体事業部内

(72)発明者 松永 和男
 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内
 (72)発明者 北川 誠
 神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所情報・通信開発本部内